PRACE NAUKOWE UNIWERSYTETU ŚLĄSKIEGO W KATOWICACH NR 12
PRACE MATEMATYCZNE II, 1972

JOANNA WUWER

O bazie dualnej do bazy potęgowej ciała

Niech E będzie rozszerzeniem rozdzielczym ciała F stopnia n, z bazą $\omega_1, \ldots, \omega_n$. Wtedy istnieje baza $\omega_1^*, \ldots, \omega_n^*$ rozszerzenia E/F, zwana bazą dualną, taka, że

$$S(\omega_i \omega_k^*) = \delta_{ik} = \begin{cases} 1 \text{ dla } i = k \\ 0 \text{ dla } i \neq k. \end{cases} \tag{1}$$

($S(a)$ oznacza tutaj ślad a w rozszerzeniu E/F).

E. ARTIN ([1], str. 89) podaje następujące

TWIERDZENIE: *Jeśli Θ jest elementem pierwotnym skończonego i rozdzielczego rozszerzenia E/F, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ — wielomianem minimalnym elementu Θ nad F, $f'(x)$ — jego pochodną, to baza dualna do bazy potęgowej $1, \Theta, \ldots, \Theta^{n-1}$ wyraża się wzorami*

$$(\Theta^{k-1})^* = \frac{1}{f'(\Theta)} \sum_{j=0}^{n-k} a_{k+j} \Theta^j, \quad k = 1, \ldots, n, \tag{2}$$

Dowód E. ARTINA opiera się na pewnej formule interpolacyjnej, pochodzącej od EULERA. W tym artykule podam inny dowód tego twierdzenia, w którym bazę dualną do potęgowej wyznacza się w sposób naturalny, wprost z definicji bazy dualnej.

Niech $(\Theta^{k-1})^* = x_{1k} + x_{2k}\Theta + \ldots + x_{nk}\Theta^{n-1}$, $x_{jk} \in F$, $k = 1, \ldots, n$. Warunki (1) dla $(\Theta^{k-1})^*$ można zapisać w postaci układu n równań liniowych o n niewiadomych $x_{1k}, \ldots, x_{nk}$:

$$x_{1k}S(\Theta^{i-1}) + x_{2k}S(\Theta^i) + \ldots + x_{nk}S(\Theta^{n+i-2}) = \delta_{ik}, \quad i = 1, \ldots, n. \tag{3}$$

Wyznacznik macierzy $A = (S(\Theta^{i+j-2}))_{1 \le i,\, j \le n}$, tego układu jest równy wyróżnikowi $D(1, \Theta, \ldots, \Theta^{n-1})$ bazy $1, \Theta, \ldots, \Theta^{n-1}$ (por. [2], str. 558), a zatem jest kwadratem wyznacznika VANDERMONDE'A $V_n = V_n(\Theta_1, \Theta_2, \ldots, \Theta_n)$, gdzie $\Theta_1, \Theta_2, \ldots \Theta_n$ są pierwiastkami wielomianu $f(x)$, $\Theta_1 = \Theta$. Wyznacznik ten jest różny od zera, gdyż elementy Θ_i ($i = 1, \ldots, n$) są parami różne, jako pierwiastki wielomianu rozdzielczego. Układ (3) jest więc układem kramerowskim, a jedyne jego rozwiązanie dane jest wzorami

$$x_{jk} = \frac{\det A_j}{\det A}, \quad j = 1, \ldots, n,$$

gdzie A_j jest macierzą powstałą z A przez zastąpienie j-tej kolumny kolumną wyrazów wolnych $\delta_{1k}, \ldots, \delta_{nk}$. Rozwijając wyznacznik macierzy A_j według j-tej kolumny otrzymamy $\det A_j = A_{kj}$, gdzie A_{kj} jest dopełnieniem algebraicznym elementu stojącego w k-tym wierszu i j-tej kolumnie macierzy A. Stąd

$$(4) \qquad (\Theta^{k-1})^* = \frac{1}{V_n^2} (A_{k1} + A_{k2}\,\Theta + \ldots + A_{kn}\,\Theta^{n-1}).$$

Zauważmy, że suma występująca w równości (4) jest rozwinięciem wyznacznika macierzy powstałej z A przez zastąpienie k-tego wiersza wierszem $1, \Theta, \ldots, \Theta^{n-1}$. Ponadto zachodzi równość

$$\det \begin{vmatrix} S(1) & S(\Theta) & \ldots & S(\Theta^{n-1}) \\ . & . & . & . \\ S(\Theta^{k-2}) & S(\Theta^{k-1}) & \ldots & S(\Theta^{n+k-3}) \\ 1 & \Theta & \ldots & \Theta^{n-1} \\ S(\Theta^{k}) & S(\Theta^{k+1}) & \ldots & S(\Theta^{n+k-1}) \\ . & . & . & . \\ S(\Theta^{n-1}) & S(\Theta^{n}) & \ldots & S(\Theta^{2n-2}) \end{vmatrix} = \det \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \Theta_1 & \Theta_2 & \ldots & \Theta_n \\ . & . & . & . \\ \Theta_1^{k-2} & \Theta_2^{k-2} & \ldots & \Theta_n^{k-2} \\ 1 & 0 & \ldots & 0 \\ \Theta_1^{k} & \Theta_2^{k} & \ldots & \Theta_n^{k} \\ . & . & . & . \\ \Theta_1^{n-1} & \Theta_2^{n-1} & \ldots & \Theta_n^{n-1} \end{vmatrix} *$$

$$* \det \begin{vmatrix} 1 & \Theta_1 & \ldots & \Theta_1^{n-1} \\ 1 & \Theta_2 & \ldots & \Theta_2^{n-1} \\ . & . & . & . \\ 1 & \Theta_k & \ldots & \Theta_k^{n-1} \\ . & . & . & . \\ 1 & \Theta_n & \ldots & \Theta_n^{n-1} \end{vmatrix}$$

skąd

$$(5) \qquad \sum_{j=1}^{n} A_{kj}\,\Theta^{j-1} = (-1)^{k+1}\, V_{n-1}^{(k-1)}\, V_n,$$

gdzie $V_{n-1}^{(k-1)}$ jest wyznacznikiem stopnia $n-1$, którego j-ta kolumna jest postaci $1, \Theta_j, \ldots, \Theta_j^{k-2}, \Theta_j^{k}, \ldots, \Theta_j^{n-1}$ $(j = 2, \ldots, n)$.

Znane są wzory (por. [3], str. 70)

$$(6) \qquad V_{n-1}^{(k-1)} = s_{n-k}(\Theta_2, \ldots, \Theta_n)\, V_{n-1}, \quad (k = 1, \ldots, n),$$

gdzie V_{n-1} jest wyznacznikiem VANDERMONDE'A, zbudowanym z elementów $\Theta_2, \ldots, \Theta_n$, $s_p(\Theta_2, \ldots, \Theta_n)$ jest p-tym wielomianem symetrycznym podstawowym zmiennych $\Theta_2, \ldots, \Theta_n$ $(s_0 = 1)$.

Podstawiając (5) i (6) do (4) otrzymamy

$$(\Theta^{k-1})^* = (-1)^{k+1} s_{n-k}(\Theta_2, \ldots, \Theta_n) \frac{V_{n-1}}{V_n} = \frac{(-1)^{k+1} s_{n-k}(\Theta_2, \ldots, \Theta_n)}{(\Theta_n-\Theta_1)\ldots(\Theta_2-\Theta_1)} =$$

$$= \frac{(-1)^{n-k} s_{n-k}(\Theta_2, \ldots, \Theta_n)}{f'(\Theta)}. \tag{7}$$

Dalej, biorąc pod uwagę związki między wielomianami symetrycznymi podstawowymi n zmiennych i $n-1$ zmiennych

$$s_p(\Theta_2, \ldots, \Theta_n) = s_p(\Theta_1, \ldots, \Theta_n) - \Theta_1 \, s_{p-1}(\Theta_2, \ldots, \Theta_n)$$

oraz wzory Viety

$$s_p(\Theta_1, \ldots, \Theta_n) = (-1)^p a_{n-p}, \quad p = 1, \ldots, n \; (a_n = 1)$$

można wyznaczyć $s_p(\Theta_2, \ldots, \Theta_n)$:

$$\begin{aligned}
s_0 &= 1 \\
s_1 &= -(a_{n-1}+\Theta) \\
s_2 &= a_{n-2}+a_{n-1}\Theta+\Theta^2 \\
&\ldots\ldots\ldots\ldots\ldots \\
s_{n-1} &= (-1)^{n-1}(a_1+a_2\Theta+\ldots+a_{n-1}\Theta^{n-2}+\Theta^{n-1}).
\end{aligned}$$

Stąd, po podstawieniu $s_{n-k}(\Theta_2, \ldots, \Theta_n) = (-1)^{n-k} \sum_{j=0}^{n-k} a_{k+j}\Theta^j$

do równości (7) otrzymamy wzory (2).

PRACE CYTOWANE

[1] E. Artin: *Theory of Algebraic Numbers*, Göttingen, 1959.
[2] L. Rédei: *Algebra*, Vol. 1, Pergamon Press, 1967.
[3] L. Jeśmanowicz i J. Łoś: *Zbiór zadań z algebry, cz. I*, Warszawa 1959.

JOANNA WUWER

ON THE DUAL BASIS TO THE 1, $\Theta, \ldots, \Theta^{n-1}$

Summary

A new proof of the theorem about the form of the dual basis to the basis $1, \Theta, \ldots, \Theta^{n-1}$ of a separable extension $F(\Theta)/F$ is given (c. f. E. Artin [1], p. 89). The basis $1^*, \Theta^*, \ldots, (\Theta^{n-1})^*$ is calculated directly from the definition of a dual basis by solving a suitable system of linear equations.

Oddano do Redakcji 2. 4. 1970 r.